IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of:)Attorney Docket No.: F-240

Douglas B. Quine   )Group Art Unit: 2622

Serial No.: 09/748,994   )Examiner: Heather D. Gibbs

Filed: December 27, 2000   )Date: September 27, 2004

Title: A METHOD FOR VERIFYING THE AUTHENCITY OF AN ELECTRONIC DOCUMENT

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL

Sir:

This is an appeal pursuant to 35 U.S.C. § 134 and 37 C.F.R. §§ 1.191 et seq. from the final rejection of claims 1-7 of the above-identified application mailed April 28, 2004. The fee for submitting this Brief is $330.00 (37 C.F.R. § 1.17(c)). Please charge Deposit Account No. **16-1885** in the amount of $330.00 to cover these fees. The Commissioner is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. **16-1885**. Enclosed with this original are two copies of this brief.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

On September 27, 2004
Date of Deposit

Signature

Elizabeth P. Czarnecki
Name

September 27, 2004
Date

REAL PARTY IN INTEREST

The real party in interest in this appeal is Pitney Bowes Inc., a Delaware corporation, the assignee of this application.

RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to Appellants, their legal representative, or the assignee that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

STATUS OF CLAIMS

The instant application was filed with claims 1-9. In the Amendment dated March 17, 2004 claims 1 and 7 were amended, and claims 8 and 9 were cancelled. In an Amendment under 37 CFR §1.116 responsive to the April 28, 2004 Final Office Action, claims 2-4 were cancelled and amendment of claim 5 was requested.

STATUS OF AMENDMENTS

Subsequent to the final rejection dated April 28, 2004, claims 2-4 and amendment of claim 5 was requested to place the application in better form for appeal. Therefore, assuming the examiner permits the amendment to claim 5, the claims as set forth in Appendix A to this brief (namely, 1, 5 and 7) are those as set after the final rejection.

SUMMARY OF INVENTION

The present claimed invention verifies the authenticity of received facsimile documents, via first and second facsimile devices, by computing an encrypted checksum of the document transmitted and comparing a decrypted checksum of the document received at the destination facsimile device with the encrypted checksum value calculated at the originating facsimile device.

The claimed present invention method provides an originating facsimile device which includes means for generating data representative of facsimile data received by the originating facsimile device and a means for computing the checksum of the facsimile data received by the originating facsimile device. The originating facsimile device further includes means for

encrypting the computed checksum, thus generating an encrypted checksum data. Means for convolving the representative data and the encrypted checksum data is also provided at the originating facsimile device in order to produce convolved data which is transmitted by the originating facsimile device to a destination facsimile device.

The destination facsimile device includes means for decrypting the encrypted checksum data and comparing the decrypted checksum data with the checksum data computed by the destination facsimile device in order to verify the authenticity of information received by the destination facsimile device. The destination facsimile device further includes means for alerting a recipient at the destination facsimile device in the event of a mismatch between the decrypted checksum data and the checksum data computed for document received by the destination facsimile device.

In summary, the present invention is directed to a method of authenticating information communicated between a first facsimile device and a second facsimile device, the information being transmitted via a communications network. In this method, the first facsimile device receives input data (physical or electronic) and generates facsimile information. The first facsimile device also calculates a checksum of the input data and encrypts the same to generate an encrypted checksum data corresponding to the received facsimile input data.

Information generated in the facsimile format is convolved with the encrypted checksum data and transmitted to a destination facsimile device. The encrypted checksum data is decrypted and compared with the checksum data calculated at the originating facsimile device in order to verify the authenticity of the facsimile data received at the destination facsimile device. The method further comprises alerting a recipient at the destination facsimile device in the event of a mismatch between the decrypted checksum data and the checksum data computed by the destination facsimile device for a document received at the destination facsimile device.

ISSUES

The issue on appeal is whether U.S. patent no. 5,982,506 to Kara (the "Kara patent") anticipates claims 1, 5 and 7 under 35 USC §102(b).

GROUPING OF CLAIMS

Claims 1, 5 and 7 are grouped together and stand and fall together.

ARGUMENT

As Appellant discusses in detail below, the final rejection of claims 1-10 are devoid of any factual or legal premise that supports the position of unpatentability. It is respectfully submitted that the rejection does not even meet the threshold burden of presenting a prima facie case of unpatentability. For this reason alone, Appellants are entitled to grant of a patent. In re Oetiker, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992).

Independent claim 1 recites a "method of authenticating information communicated between a first facsimile communication device and a second facsimile communication device. . . " Thus, the intended environment of use for the present invention is facsimile devices. For the reasons set forth below, the teachings of the Kara patent are not applicable to facsimile devices and certainly do not anticipate the recited facsimile features of the present claimed invention.

Regarding the Kara patent, the examiner states it relates to a facsimile device merely by making reference to Kara's background at Col. 1, lines 5-20. However, a proper reading of this section, and the overall teaching of the Kara patent, reveals that mention of a facsimile device in it's background is only provided as a historical reference to how the electronic transfer of documents evolved, starting with facsimile devices. After this background recital, the Kara patent never again mentions facsimile devices and actually specifically teaches of using personal computers (PC's) for implementing its inventive document certification system and method. See figs. 1 and 2 of the Kara patent depicting the preferred and alternative embodiments for performing document certification using at least a recipient and sender's PC (10 and 20) as does the entire specification of the Kara patent. Again, other than mentioning "facsimile" in its background for historical purposes, the Kara patent never again mentions or teaches using facsimile communication or devices for its inventive system and method. An explanation as to why the teachings of the Kara patent are not applicable to facsimile devices is set forth below.

As now explained, expanding the scope of the Kara patent beyond PC's to that of facsimile devices would destroy the teachings of the Kara patent. A proper reading of the Kara patent reveals that it teaches a system and method for generating a "certification indicia" either in an secure PC 30 or a receiver's PC 20. This certification indicia embeds "the checksum of the encrypted electronic document, date and time of receipt by the recipient, number of pages in the document, identification of the recipient, and identification of the sender. This indicia is then transmitted to the sender's PC for proof of certified transmission of an electronic document." (See. Col. 5, lines 15-22 of the Kara patent). And as shown in figures 6A to 6C of the Kara patent, this "certified indicia" is actually evidence of postage to be applied by the user of the sender's PC (10) to preferably a mailpiece, via a coupled external printer. Preferably, the "certified indicia" is what is known as a security packet (i.e., postage), and is actually transmitted back to the sender's PC (10) so as to be reproduced in a machine readable bar code format, like what is depicted in Figs. 6A to 6C. Hence, this "certified indicia" can then be applied to documents (i.e., mailpieces) so as to be later verified by proper verifying equipment (i.e., postal bar code readers). See Col. 25, line 63 to Col. 26, line 67 of the Kara patent.

Referring now to the present claimed method of authenticating information between facsimile devices, its facsimile claim recitations are certainly not disclosed, suggested nor taught by the Kara patent because expanding Kara to teach of facsimile devices would clearly destroy its teachings. Simply put, there is no reason why a facsimile device would be used to generate indicia to be applied to another document, such as a mailpiece. It is not even known to the assignee of the present invention (e.g.. Pitney Bowes Inc.) who is a leader in the postal industry how one skilled in the art would apply the certified indicia generated by a facsimile device to a such another mailpiece. This clearly demonstrates why the Kara patent only relates to PC's coupled to external printers in all its disclosed embodiments.
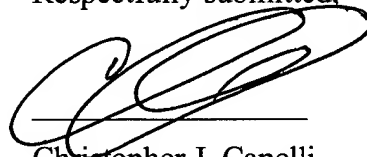
Applicant acknowledges the Merriam-Websters Collegiate Dictionary (10th ed) definition for "facsimile" (as set forth by the Examiner) and states while it may be conceptual correct, it is also the broadest possible definition for "facsimile", which definition is certainly out of context when applied to the present claimed invention.

5

Accordingly, independent claim 1, along with its depending claims (namely, 5 and 7) patentably distinguish from the Kara patent and it is respectfully submitted removal of this rejection is warranted.

CONCLUSION

In Conclusion, Appellants respectfully submit that the final rejection of claims 1, 5 and 7 is in error for at least the reasons given above and should, therefore, be reversed.

Respectfully submitted,

Christopher J. Capelli
Reg. No. 38,405
Attorney for the Appellants
Telephone (203) 924-3849

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, Connecticut 06484-8000

{I0030799.1 }

APPENDIX A

Claim 1: A method of authenticating information communicated between a first facsimile communication device and a second facsimile communication device via a communications network, comprising the steps of:

    a. receiving input data and generating facsimile information in a first format by said first communication device from said input data;

    b. processing said input data to compute an encrypted checksum;

    c. convolving said facsimile information with said encrypted checksum data to produce convolved data;

    d. decrypting, at said second communication device, said encrypted checksum ;

    e. computing a checksum of said input data received at said second communications device; and

    f. alerting a recipient at said second communication device in the event of a mismatch between said checksum data computed in step (e) and said decrypted checksum data in step (d).

Claim 5: The method of claim 1, wherein a database system is communicatively coupled to said second facsimile communication device.

Claim 7: The method of claim 1, further comprising the step of configuring an e-mail system for receiving and displaying an alert message to said recipient along with said received input data.